Software Maintenance Release Note

Version 89273-02 for AT-8900 and AT-9900 series switches

Introduction

This release note lists the issues addressed and enhancements made in version 89273-02 for Software Release 2.7.3 on existing models of AT-8900 and AT-9900 series switches. File details are listed in Table 1.

Table 1: File details for version 89273-02.

Base Software Release File	89-273.rez
Release Date	29 April 2005
Compressed File Name	89273-02.rez
Compressed File Size	4263880 bytes

This release note should be read in conjunction with the following documents:

- Release Note: Software Release 2.7.3 for AT-9900, AT-8900, SwitchBlade, AT-9800, AT-8800, Rapier, Rapier i, AT-8700XL, and AT-8600 Series Switches and AR400 and AR700 Series Routers (Document Number C613-10431-00 REV A) available from *www.alliedtelesyn.com*
- AT-8900 series switch Documentation Set for Software Release 2.6.2 available on the Documentation and Tools CD-ROM packaged with your switch, or from *www.alliedtelesyn.co.nz/documentation/documentation.html*.
- AT-9900 series switch Documentation Set for Software Release 2.6.6 available on the Documentation and Tools CD-ROM packaged with your switch, or from *www.alliedtelesyn.com*.

WARNING: Using a maintenance release for a different model or software release may cause unpredictable results, including disruption to the network. Information in this release note is subject to change without notice and does not represent a commitment on the part of Allied Telesyn International. While every effort has been made to ensure that the information contained within this document and the features and changes described are accurate, Allied Telesyn International can not accept any type of liability for errors in, or omissions arising from the use of this information.

Some of the issues addressed in this Release Note include a level number. This number reflects the importance of the issue that has been resolved. The levels are:

Level 1 This issue will cause significant interruption to network services, and there is no work-around.

Level 2 This issue will cause interruption to network service, however there is a work-around.

Level 3 This issue will seldom appear, and will cause minor inconvenience.

Level 4 This issue represents a cosmetic change and does not affect network operation.

Enabling and installing this Release

To use this maintenance release you must have a base release license for Software Release 2.7.3. Contact your distributor or reseller for more information.

To enable this release and install it as the preferred release, use the commands:

```
enable rel=89273-02.rez num=2.7.3
set install=pref rel=89273-02.rez
```

Features in 89273-02

Patch 89273-02 includes the following enhancements and resolved issues:

Level 1

CR00005227 Module: SWI, RSTP, SWMX, SWCX, SW56 Level: 1

A heavy processor load could lead to queuing RSTP BPDUs, which in turn could lead to even more processor load, resulting in more queued BPDUs. This issue has been resolved by improving the efficiency in the interaction between RSTP TCN BPDUs and the hardware tables.

This issue has been resolved. (PCR number: 40672)

CR00006609 Module: LB Level: 1

When failover occurred between a redundant pair of Load Balancing devices, host ARP caches were not updated with the new Master's MAC address, thus causing the hosts to lose connectivity until their ARP caches timed out the stale entry. This issue has been resolved. (No PCR number.)

CR00007034 Module: Firewall Level: 1

A reboot could occur while ageing out Firewall sessions when the device was under heavy load and had many active Firewall sessions.

This issue has been resolved. (No PCR number.)

CR00007695 Module: PPP Level: 1

When either the Firewall was enabled or multiple L2TP tunnels were configured, and a default route existed over an L2TP tunnel, it was possible for an infinite internal packet loop to be created when a packet was sent over the L2TP tunnel after the underlying interface route to the remote IP had gone down. This caused a reboot to occur.

This issue has been resolved. (No PCR number.)

Level 2

CR00002290 Module: STP, SWI Level: 2

Previously, the forwarding database was flushed instead of being aged out when an STP topology change notification was received.

This issue has been resolved. (PCR number: 40185)

CR00002662 Module: STP Level: 2

Previously, when a port or ports was moved from one VLAN to another, the switch would reset both STP/RSTP instances that control the VLANs. This behaviour is now changed to only reset the STP process on the STP instance that the port(s) is joining. The switch will now also retain the port(s) edge-port setting during the moving process.

This issue has been resolved.

CR00004964 Module: CORE, PSS, QOS, SWI SWMX, Level: 2

A switch, lock-up could occur after enabling the use of QoS Counters via the command SET SWITCH ENHANCEDMODE=QOSCOUNTERS.

This issue has been resolved.

CR00005983 Module: IPNAT Level: 2

When IP NAT was configured, a restart could occur if a TCP RST packet was received with flags in addition to ACK.

This issue has been resolved.(PCR number: 40728)

CR00006521 Module: IPv6 Level: 2

The "SET IPV6 MLD ?" command was not displaying the correct parameters on the command-line.

This issue has been resolved.

CR00006554 Module: PPP Level: 2

PPP TCP mss clamping was always fixing the mss to 1372. This issue is now fixed, so that if the MTU or MRU is less than 1472, then mss clamping clamps the mss to the correct size.

This issue has been resolved.

CR00006769 Module: PPP Level: 2

PPPoE has been modified so that a single host can be attached to multiple access concentrators without a conflict of session ID's.

CR00007005 Module: PPP Level: 2

A change was made in the 2.6.1 software release to reset the PPP idle timer for received traffic as well as transmitted traffic to avoid a PPP link idling out when receiving unidirectional traffic. However, this has undesirable side effects as it is not possible to control the received traffic. This change has been removed. Users can avoid a PPP link idling out for received unidirectional traffic by setting the value of the IDLE parameter to OFF, or in the case of received multicast traffic, setting the IDLE parameter to a value greater than the multicast hello timer.

CR00007078 Module: PPP Level: 2

When PPP was configured over L2TP over PPPoE, and the firewall was enabled, a restart could occur in some circumstances.

This issue has been resolved.

CR00007291 Module: IPG Level: 2

If RIP was configured to explicitly exchange packets with a neighbour in another subnet, the RIP packets from that neighbour were dropped.

This issue has been resolved.

CR00007341 Module: IPG Level: 2

When routers and switches were using CIDR addressing, with a unicast address coinciding with a network broadcast address of class A, B, or C, then they could incorrectly forward traffic as directed broadcasts, even though the traffic was unicast (only).

This issue has been resolved. (PCR number: 50069)

CR00007436 Module: L2TP Level: 2

When the router was acting as an L2TP Access Concentrator (LAC) it would fail to negotiate a Virtual tunnel to another vendor's LNS. This was due to invalid Proxy LCP AVPs being used within the ICCN message.

This issue has been resolved. (No PCR number.)

CR00007477 Module: SWMX Level: 2

In some 8924/9924 network configurations deploying QoS and IPMC traffic, the QoS may have periodically miss-classified the traffic.

This issue has been resolved.

CR00007493 Module: FIREWALL Level: 2

When the firewall was configured and the firewall ident proxy feature was disabled, or if the firewall was disabled, TCP port 113 was still left open.

This issue has been resolved.

CR00007605 Module: SWMX, PSS Level: 2

QoS was incorrectly misclassifying packets for small periods of time.

This issue has been resolved

CR00007888 Module: OSPF Level: 2

NSSA areas were not able to form adjacencies with some other vendors' equipment.

This has been resolved.

CR00007948 Module: SSH Level: 2

Some SSH Clients do not limit the length of the SSH username. Under some special circumstances, when the AlliedWare ™ SSH server received a username of 186 characters, the device would restart unexpectedly. This was fixed to limit a SSH username to be less than 64 characters and returning a failure message if the username was 64 or more characters.

CR00007991 Module: FIREWALL Level: 2

Restarts could occur when the firewall parsing process was searching for the character '/' in a string.

This issue has been resolved.

CR00007992 Module: SSH Level: 2

Under some circumstances the SSH listen port would be closed.

This issue has been resolved.

CR00008008 Module: Firewall Level: 2

Add firewall policy list would overwrite the low memory 0x0.

This issue has been resolved.

CR00008068 Module: HTTP Level: 2

When a URL contains an IP address instead of a Domain name and the inverse DNS lookup for resolving the domain name failed, the proxy server could block the cookies incorrectly. Also the Proxy server could parse an HTTP message incorrectly if the URL field of the HTTP message contained non-ASCII characters.

These issues have been resolved

CR00008080 Module: TRG Level: 2

Triggers based on memory resource were not activated when the specified memory level was reached.

This issue has been resolved.

CR00008101 Module: FILE Level: 2

The COPY command returned an error message saying the input filename was invalid, even if a valid filename was given.

This issue has been resolved

CR00008117 Module: IPG, VRRP Level: 2

ARP requests received that matched a static ARP entry would overwrite the hardware switching tables for that entry. The static ARP in software (SHOW IP ARP) would remain as defined by the user, however. Now, if an ARP

entry has been added statically, the hardware switching tables are not updated by the dynamic ARP information.

CR00008176 Module: FFS, FILE Level: 2

The flash file system could sometimes have duplicate copies of a file.

This issue has been resolved.

CR00008184 Module: IPG Level: 2

If an IP interface was assigned its IP address dynamically, and the IP that it was assigned matched the Network address of another interface on the device, then the device would drop packets destined for the remotely assigned IP interface.

This issue has been resolved. PCR40549

CR00008266 Module: CORE Level: 2

A reboot could occur if a device had an extremely large boot script.

This issue has been resolved

Level 3

CR00007476 Module: IPG Level: 3

The DNS relay has been changed to allow the relay of resource record types between 0x1d and 0xff. Previously packets with these types of resource records were dropped.

This issue has been resolved (No PCR number.)

CR00007521 Module: IPG Level: 3

DVMRP packets were being dropped due to packet length inconsistencies from other vendor devices.

This issue has been resolved. (No PCR number.)

CR00007716 Module: LOG Level: 3

Previously, when changing the password on a log output/receive definition to a shorter string, the log message exchange could fail.

This issue has been resolved. (PCR number: 50070)

CR00008098 Module: CORE, SWMX Level: 3

A slight change has been made to the Mirror ports tagged mode. If all mirroring ports are untagged then the Mirror port will transmit only untagged packets. If at least one mirroring port is tagged then the Mirror port will always transmit tagged packets.

Previously, the Mirror port would always transmit tagged packets regardless of the mirroring port(s) tagging mode.

CR00008123 Module: SWI Level: 3

The 9924/8948 could reboot when attempting to display the ASIC LED control register.

This issue has been resolved

Level 4

CR00006093 Module: FFS Level: 4

There was not enough information displayed to the user when the ACTIVATE FLASH COMPACTION command was entered at the same time as Flash was compacting.

This issue has been resolved. (No PCR number.)

Enhancements

CR00006652 Module: IKMP, IPSEC

Previously ISAKMP NAT-T was enabled by default on every ISAKMP policy created. NAT-T is now disabled by default on every ISAKMP policy. (No PCR number.)

CR00006953 Module: PPP

The ability to configure Van Jacobson Header Compression over dynamic PPP interfaces has been added. To this end, the command parameter 'VJC={ON | OFF}' has been added to the CREATE and SET PPP TEMPLATE commands. (No PCR number.)

CR00008045 Module: SWMX

Add support for the MG8T (Agilent QBCU-5730R) to support 10/100/1000 modes of operation.

CR00008367 Module: FIREWALL

Support has been added for VoIP services using SIP (port 5060) where the VOIP phone's session setup is 5 packets or less and the keepalive is greater than 5 min.

Note: If the keepalive is greater than the default udpTimeout of 20 minutes, then this will need to be configured for the firewall policy.

Features in 89273-01

No release.